13 August 2018

[EBF_Ref 033346]

EBA CONSULTATION PAPER: Draft guidelines on the conditions to be met to benefit from an exemption from contingency measures under article 33 (6) of Regulation (EU) 2018/389

Question 1: Do you agree with the EBA's assessments on KPIs and the calculation of uptime and downtime and the ASPSP submission of a plan to publishing statistics, the options that EBA considered and progressed or discarded, and the requirements proposed in Guideline 2 and 3?

If not, please provide detail on other KPIs or calculation methods that you consider more suitable and your reasoning for doing so

The European Banking Federation (EBF) and its members are overall supportive of EBA's assessments on KPIs and the calculation of uptime and downtime. However, we have some comments on some technical details.

- EBF members understand that ASPSPs will designate their dedicated interface as a critical business process - as they already do for the customer interface/proprietary channel. Therefore, the dedicated interface will be subject to the same high standards of uptime and availability as an online banking interface.
  In this context, Key Performance Indicators (KPIs) to monitor the performance of the dedicated interface, as detailed in the guidelines, will not necessarily match with the KPIs currently in use to monitor the availability and performance of Payment Service User (PSU) channels (eg online banking) as provided by an ASPSP.
  In this context, comparison of availability and performance (referenced **in paragraph 24**) should be at channel level i.e. the channel chosen by the client. It is not appropriate to compare the API availability and performance with the best performing PSU interface, because:
  - By definition, a mobile banking interface will usually have a different access scope compared to the fully-fledged online banking interface. The first might allow only a limited access to the account and to limited types of transactions considered more appropriated for the user compared to the full online banking interface
  - Service levels and availabilities for interfaces differ by client profile based on customer's targets and individual service level agreements – this is specifically the case for commercial clients

  These differences should be taken into account in the monitoring approach adopted. Each ASPSP channel/segment has its own SLA/KPI, therefore the comparison of the API performance can be done only with the specific channel/segment which should be selected by the ASPSP based on the brand/channel.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

- Against this background, if the EBA would like to specify some high-level metrics which could be applied across the industry, the EBF suggest the following:
    - Number of critical impacts and incidents, (outage based on a monthly figure) underpinned by a series of service levels including serviceability (unplanned disruption), availability (planned service disruption), the service support
    - Number of critical impacts longer than 120 minutes
    - Total outage time as regards incidents
    - Mean recovery time as regards incidents
    - Performance service levels such as page load time targets, sign off/sign on targets.

- In light of the above, also the concept of 'accuracy of information provided' (**paragraph 21**) should be interpreted as to refer to the accuracy of KPIs.

- **Guideline 2.3:** We understand that when confirmation of funds via yes/no message cannot be provided by the ASPSP, the additional information to be provided are limited only to what is needed for the execution of the payment. Allowing access to any other data would be against requirements on data minimisation or consent.

- **Guideline 2.4. :**
    - The service level should be measured over a longer time period rather than each 24-hour period, to provide a more reliable metric.
    - The reference time period is important to ensure that the dedicated interface is subject to high standard, and possible "underperformance" is not triggered inappropriately or unnecessarily, particularly taking into account the reality of unexpected downtime. Unexpected downtime could possibly affect the dedicated and user interfaces at different moments (i.e. in different 24-hour periods). In such case the dedicated interface could register "under-performing" metrics in a 24-hour period while it could even significantly exceed the user interface service levels over a longer time horizon. The use of a longer time span would help reducing the number of "false positives".
      Therefore, we suggest amending the guidelines according to the following proposal: "a. calculate the percentage planned and unplanned downtime by using the total number of seconds the dedicated interface was down in a period ***of three months*** starting and ending ***on day one of each quarter*** at midnight".

    - There is also a need to ensure that any form of manipulation where, for instance, an external party has deliberately overloaded an API, is included in the unplanned downtime parameter in both 2.2(c) and 2.4(b). Also, planned downtimes should not be considered in 2.4.b and c.

    - Likewise, if a request is blocked or deleted at transmission level due to IP technical problems or internet provider problems, the performance of the ASPSPs dedicated interface cannot be questioned.

    - In line with the service level targets measurement, the dedicated interface should be calculated as an "average" performance value.

- **Guideline 3:**

- We would like to express our concerns regarding the publication of service level information on all ASPSP's other user interfaces. This information is sensitive as reveals competitive information, thus it should not be publicly available. The publication of absolute value statistics would allow a comparison of the performance of each ASPSP towards its customers, which is not only commercially sensitive, but would also favour cyberattacks. If a bank would be exposed to, for instance, a Distributed Denial of Service (DDoS) attack; the effects of such an attack would then be included in the publication, potentially putting at risk the cybersecurity infrastructure of the bank. The institutions behind the attack are then able to evaluate the success of their actions and adapt their processes thereafter. It should also be considered that such requirement seems to go beyond the scope and spirit of the Guidelines, whose aim is to allow NCAs to assess whether the performance of the dedicated interfaces towards TPPs is equivalent to the user interface, and not to disclose the relationship between ASPSPs and their clients.
  Also, the definition of "down" for the user interface is not clearly defined and there are likely to be substantial differences in interpretation among different ASPSPs. This could generate confusion and inappropriate comparisons. For example, some ASPSPs might consider their user interface to be "down" if one specific functionality is not working, while another may only define their interface as down if the entire system is offline.
  We would therefore suggest considering this requirement as restricted to publishing percentage values comparing the availability of the user interface and the dedicated interface. As a result, ASPSP's should only be obliged to report service level information on their dedicated interface to their Competent Authority ex post, together with the reporting of the other relevant service levels, permitting Authorities to confirm their compliance with the RTS and Guidelines.

  Therefore, we suggest amending Guideline 3.1 according to the following proposal:
  For the purpose of Article 32(4) of the RTS, the ASPSP should ***report*** *to its competent authority:*
- ~~*statistics*~~ ***percentage*** *on a quarterly basis on availability and performance as set out in Guideline 2.2 and 2.3 for the dedicated interface and each payment service user interface together with information on where these* ***percentage*** *statistics will be published and the date of first publication****. Access to further information shall be restricted to Competent Authorities****; and*
- *from the date of first* ***reporting, informing the Authority of*** *the comparison of the availability of its dedicated interface with* ~~*its best performing*~~ ***the*** *PSU interface*

Question 2: Do you agree with the EBA's assessments on stress testing and the options it considered and progressed or discarded, and the requirements proposed in Guideline 4? If not, please provide your reasoning.

We agree with the proposal of not explicitly include testing (such as security and penetration testing) that is already part of an IT assessment.

Question 3: Do you agree with the EBA's assessments on monitoring? If not, please provide your reasoning

We do agree with the assessment that monitoring by CAs cannot be considered a criterion for granting an exemption to an ASPSP and it should be limited to compliance.

Question 4: Do you agree with the EBA's assessments on obstacles, the options it considered and progressed or discarded, and the requirements proposed in Guideline 5? If not, please provide your reasoning.

- The EBF welcomes the EBA's clarification regarding obstacles and agrees in principle with the EBA assessment – notably, with the assessment that 'redirection' is not in itself an obstacle. However, we suggest reviewing the authentication terminology in the Guidelines to improve clarity and ensure consistency with the EBA Opinion.
  In particular, Guideline 5.1 a. refers to '**method of access'** to address what the EBA opinion of 13 June instead refers to as '**authentication procedure**' as per the '*methods of carrying out authentication procedure of the PSU trough a dedicated interface, and API in particular, namely redirection, embedded approach, and decoupled approach'*. To ensure legal certainty, we suggest using similar language in the Guidelines as in the Opinion, e.g. refer to: methods for carrying out the authentication procedure.

Question 5: Do you agree with the EBA's assessments for design and testing, the options it considered and progressed or discarded, and the requirements proposed Guideline 6? If not, please provide your reasoning.

- We agree with the EBA's assessments for design and testing. We believe that a testing environment should be based on what is commonly called 'conformance testing', or 'compliance testing'. Conformance testing verifies that a product performs according to its specified standards and is commonly used and determines whether a process, product, or services complies with the requirements of a specification, technical standard, contract, or regulation. Conformance Testing can be logical or physical, and it comprises the following types of testing:
  - Compliance Testing
  - Load Testing
  - Stress Testing
  - Volume Testing

  It allows for firms to either test themselves on a 'self-attestation' basis or for independent firms to review the testing. We also believe that API initiatives should provide the tools or basis for this testing based on strong collaboration with the industry. A firm can then provide to the NCA their test results to gain an exemption.

- **Paragraph 52/53:** It should be explicitly mentioned also in the text of the guidelines that testing is performed on a dedicated test environment for which service levels differ from production or live environment.

- We acknowledge that article 30.5 requires testing when applications are still pending. However, mindful of the impact that this requirement may have on the ability for an ASPSP to innovate, if any innovation by the ASPSP must always be made available to all the TPP's before the actual introduction into the market, we think that TPP should at a minimum have a compliant certificate to start testing. Also, the availability of the technical specifications before authorisation should be reconsidered to avoid unnecessary diffusion of elements that could result in a fraudulent behaviour or attempts from non-authorised PSPs to access customers' payments accounts.

- **Guideline 6.2 (f)**: We understand that when confirmation of funds via yes/no message cannot be provided by the ASPSP, the additional information to be provided are limited only to what is needed for the execution of the payment. Allowing access to any other data would be against requirements on data minimisation or consent.

Question 6: Do you agree with the EBA's assessment for 'widely used', the options it considered and discarded, and the requirements proposed Guideline 7? If not, please provide your reasoning.

- **Paragraph 55-59**: We support the EBA's assessment that the requirement 'widely used' is difficult to assess prior to 14 Sept 2019 and it should also be specific to each Member State. We welcome the alternative proposal for this specific period for ASPSPs to prove/document the measures taken to publicise and encourage testing and usage of the API. Whilst it is the intention of ASPSPs to have the API up for testing well in advance of the minimum testing period, it is clearly beyond an ASPSPs direct influence upon TPP to make use of this testing environment as well as production interface prior 14 Sept 2019.

- **Guideline 7.1** : We would like to stress that to comply with guideline 7.1. certificates for the testing phase are needed.

- **Guideline 7.2:** We would suggest that the evidence ASPSP are requested to provide is limited to publications on the ASPSPs' websites or channels. The other ways of publicising their interfaces should clearly be indicated as further options left to the policy of each individual ASPSP. We also understand that if the APIs are available for functional testing within the Test Facility, this will meet the criteria for Guideline 7.

Question 7: Do you agree with the EBAs assessment to use the service level targets and statistical data for the assessment of resolving problems without undue delay, the options it discarded, and the requirements proposed Guideline 8? If not, please provide your reasoning.

- We support the EBA's assessment that the condition for the sufficient resolution of problems is to be seen in the context of testing. However, documents supporting GL 8.1 should be part of the ASPSP's application for exemption.

Question 8: Do you agree with the proposed Guideline 9 and the information submitted to the EBA in the Assessment Form in the Annex? If not, please provide your reasoning.

- We support EBA's pragmatic approach and welcome the temporary provisions to ensure a timely processing of exemption requests prior to Sept 2019. Nevertheless, from our point of view, the mechanism to oppose a negative decision should also be described and harmonized by the Guidelines. There should be clear timelines for acknowledgement and response of the exemptions, especially given the short deadlines which are imposed on both NCAs and the industry.

- We would also welcome a reference in the guidelines that ASPSPs who implement one API for TPP access across PSU interfaces in multiple countries or clients (e.g. retail vs corporate customers) will only have to apply for the exemptions for that API once with the NCA in the Member States where it has its registered head office, as clarified during the hearing on the consultation.

Question 9: Do you have any particular concerns regarding the envisaged timelines for ASPSPs to meet the requirements set out in these Guidelines prior to the September 2019 deadline, including providing the technical specifications and testing facilities in advance of the March 2019 deadline

- We support the EBA definition of the envisaged timelines. However, we are very concerned about the process and envisaged timelines for ASPSPs to develop an API and more specifically, the possibility for CAs to assess whether or not the ASPSPs meet the requirements for an exemption according to article 33.6 in the RTS. Time is very short considering also that the PSD2 has not been transposed in all Member States yet and certificates are not in place, therefore that part of the dedicated interface cannot be finalised nor tested. An ASPSP must be ready to publish the documentation on their websites already in the beginning of 2019 to meet the deadline in September 2019. There is still an uncertainty on the administration time for local CAs which makes it difficult to understand and take into account the timelines for applications. This is especially important as any rejected exemption application leads to the need for develop a fall-back solution in two months' time.

Question 10: Do you agree with the level of detail set out in the draft Guidelines as proposed in this Consultation Paper or would you have expected either more or less detailed requirements on a particular aspect? Please provide your reasoning.

- We agree with the overall level of detail.
- Additionally, we would like to stress that there is need for certificates for the test phase in order to comply with the guidelines. The timing issue is pressing and of high concern.

About the EBF:

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

For more information contact:

Noémie Papp

Head of Digital & Retail

n.papp@ebf.eu

+32 2 508 37 69

Lucia Pecchini

Policy Adviser

l.pecchini@ebf.eu

+32 2 508 37 26